Remarks

Status of application

Claims 1-47 were examined and stand finally rejected in view of prior art. The Examiner's courtesy of a telephone interview on February 23, 2010 is appreciated. Further to that interview, Applicant faxed a claim amendment proposal (to be filed via Supplemental Amendment upon Examiner's approval). Instead of receiving any sort of response to the proposal, Applicant received a Final Rejection. In a follow-up conversation with the Examiner, Applicant's representative was informed that the best means to have the proposal now considered is through an Amendment After Final. Thus, Applicant now files same and respectfully requests re-examination and reconsideration.

The invention

For a brief statement of Applicant's invention, please refer to the last-filed Appeal Brief.

Prior art rejections

A. Section 103: Aaron and Ablay

Claims 1-47 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Aaron et al. (US 7,509,675, "Aaron") in view of Ablay et al. (US 6,002,941, "Ablay").

Aaron describes a "non-invasive monitoring of the effectiveness of electronic security services." Aaron's described system includes a test generation engine for generating and launching a denatured attack towards a customer's network. A monitoring and evaluation agent is operatively coupled to the test generation engine and is adapted to monitor and evaluate the denatured attack. A recording and analysis engine is adapted to record and analyze the results of the denatured attack. The focus of Aaron's system is his test generation engine (TGE) 36. The TGE 36 generates and launches test attacks over the network toward the monitored customer's network, with the attacks being monitored and evaluated by a monitoring and evaluation agent (MEA) 34. The attacks are "denatured" meaning the attack has been rendered harmless but remains in a format as close as possible to an actual attack so that the attack resembles an actual attack. As described, Aaron's system is not even a security system but instead a system to test the effectiveness of one's pre-existing security system. As such, Aaron appears far less relevant than previously relied-upon Teal (which the Examiner now abandons). Simply put, Aaron cannot possibly replicate Applicant's security system features as Aaron "ain't even" a security system, but instead simply a system to generate attacks to see if some other pre-existing security system is working (i.e., can detect Aaron's fake attacks).

Applicant's invention is a security system ("Security System with Methodology for Interprocess Communication Control") providing methods that control an unauthorized application's ability to gain **indirect access** to the Internet or other computer networks. As noted in Applicant's Specification, a malicious application is able to gain indirect Internet access by nefarious means: masquerading its activities by going through an operating system service or other application authorized for Internet access. This leads to a security breach that is undetectable by prior art security systems. Those systems simply see the (direct) Internet access by the operating system or authorized application. They fail to look behind the scene to see that this (direct) Internet access by the operating system or authorized application is in fact at the behest of an unauthorized application -- one that is obtaining indirect Internet access by using the operating system or authorized application as a proxy or surrogate for network access. In Applicant's previous and current amendments, the claims were revised to explicitly highlight this distinction: the revised claim language is directed to detecting and thwarting an unauthorized application's attempt at gaining network access (e.g., Internet access) through indirect means (i.e., masquerading its activities by going through an operating system service).

Applicant's prior and current amendments highlight Applicant's protection against unauthorized indirect access. Applicant has carefully reviewed Aaron but is unable to find disclosure related to detecting and thwarting an unauthorized application's ability to gain indirect access to the Internet or other computer networks. Aaron discusses the fact that attacks can be "indirect" (although little detail is provided). As set forth in Applicant's Background section, attacks via indirect access are (well) known to exist as a problem. Applicant does not claim to have invented the problem (attacks via indirect access) but instead claims to have invented a solution (security system that detects detects and thwarts attacks via indirect access). The relevance of Aaron cannot be understood, outside Aaron's overlap with Applicant's Background section (that indirect attacks are an existing problem).

Ablay for its part appears largely unrelated (if not irrelevant) to personal computer security systems such as previously relied upon Teals's security system or Applicant's security system. To the extent that the Examiner believed Applicant's prior claims were so broad as to read on unrelated art such as Ablay, it is submitted that the amended claims cannot be interpreted with such breath. Neither Aaron nor Ablay have any teaching or other relevant disclosure related to detecting and controlling indirect access to a computer network or the Internet by a rogue application.

Applicant's claims set forth a patentable advance in the area of controlling network access of potentially "bad" applications or processes that may compromise computer security through indirect access means. In view of the clarifying amendments and remarks made herein, it is respectfully submitted that the claims distinguish over the combined references and any rejection under Section 103 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at (408) 884 1507.

Respectfully submitted,

Date: July 14, 2010

/John A. Smart/

John A. Smart; Reg. No. 34929
Attorney of record

201 Los Gatos - Saratoga Rd #161
Los Gatos, CA 95030-5308
(408) 884 1507
(815) 572 8299 FAX